

Remote Access Test

If your organisation relies on Virtual Private Networks (VPN) and Remote Access Services (RAS) to provide secure communication channels over public networks to your employees and customers, do you know exactly where the security issues lie within these systems?

IRM's Remote Access Test evaluates the security of all the components making up that environment using proven methodologies to assess the security of the architecture. The result is a comprehensive understanding of vulnerabilities and exposures that might help an external attacker gain access to your internal network.

IRM will assess the configuration of all VPN endpoints and tunnels, as well as RAS implementations. This will highlight possible risks and exposures related to the design and implementation of these communication channels, where compromise would allow an attacker to gain access to sensitive information such as customer data.

A complete Remote Access Test includes the following phases:

- **Environment Mapping**

Information about all devices involved as part of the secure communication channels will be gathered, from establishment of the tunnels to the encryption and data flow mechanisms. This information is gathered through manual and automated assessments, using tools such as port and vulnerability scanners.

- **Component Analysis**

Each component of the identified devices will be evaluated with a view to understanding the correct operation of each element. Each identified element will also be considered in detail within the wider context of the environment as a whole.

- **Vulnerability Identification and Analysis**

The security requirements of the VPN/RAS presence are assessed, identifying potential vulnerabilities in the gaps between the requirements and the implementation. The following are considered core components of this analysis yet other areas of interest may be considered as appropriate to the architecture in question:

- Authentication assessment
- Security of access to data
- Administration interfaces
- Strength of encryption
- VPN client configuration
- Tunnel implementation

- **Internal Network Review**

Optionally, IRM can supplement the Remote Access Test with a review of the internal network, where the extent of access to internal systems and services that an attacker could achieve having gained access to the remote access system will be enumerated.

- **Deliverables**

IRM will deliver a formal report including an executive summary, a risks and recommendations table detailing the high level results of the assessment and a detailed description of each issue discovered including remediation advice.

About IRM

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.